Notice of Allowability	**Application No.** 10/829,176	**Applicant(s)** BOULANGER ET AL.	
	Examiner Joseph E. Avellino	**Art Unit** 2143	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *RCE dated 9/28/07 and Interview summary dated December 12, 2007*.

2. ☒ The allowed claim(s) is/are *1,7-41,43-47 and 49-51*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
   1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *herewith* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Patrick Daugherty on December 12, 2007.

The application has been amended as follows:

Please amend the TITLE as follows:

~~Method, program and for~~ Automatically detecting malicious computer network reconnaissance by updating state codes in a histogram.

Please amend the CLAIMS as follows:

1. (Presently Amended) A method to detect unauthorized reconnaissance or scanning of a computer network comprising ~~the acts of~~:

monitoring communications within the network;

detecting a predefined sequential triplet of TCP/IP protocol set packets flowing within said communications, each of the predefined sequential triplet packets comprising a source address field, a target device address field, a source port field and a target device port field, comprising ~~the steps of~~:

providing a histogram in which states of the predefined sequence of packets are maintained, the histogram including a table partitioned into a first field in which source addresses of network devices are kept and a second field concatenated to the first field;

dynamically updating said histogram as selected ones of the predefined sequence of packets is detected by initializing or incrementing a state code field in response to an order in which packets in the predefined sequence of packets are detected; concatenating a source address field, a target device address field, a source port field and a target device port field of a packet of the predefined sequential triplet into the table first and second fields as an ordered four-tuple; hashing the ordered four-tuple; and using the hashed ordered four-tuple as a histogram location index;

observing an initial SYN packet originating from a source address;

detecting a next sequential SYN/ACK packet issuing from a target device address in response to the SYN packet; and

detecting a last sequential RST packet originating from the source address in response to the SYN/ACK packet; and

issuing an alert indicating unauthorized scanning if the predefined sequence of packets are each relevant to the source address and if the state code field has an alert value.

Claims 2-7. (Cancelled)

8. (Currently Amended) The method of claim [4] 1 wherein the issuing further includes sending a message to an administrator.

9. (Currently Amended) The method of claim [4-] 1 wherein the issuing further includes blocking future packets comprising the source address, the target device address and a target device port address.

10. (Currently Amended) The method of claim [4] 1 wherein issuing further includes rate-limiting flows of packets comprising the source address.

11-24. (Cancelled).

25. (Presently Amended) A method to deploy an intrusion detection system on a network device ~~including acts of~~ comprising:

providing an algorithm to detect a predefined sequential triplet of TCP/IP protocol packets;

providing a table to record at least one characteristic to identify network devices and state code corresponding to a sequence in which the predefined sequential triplet of packets are received, wherein each of the predefined sequential triplet packets comprise a source address field, a target device address field, a source port field and a target device port field;

dynamically updating a histogram byconcatenating a source address field, a target device address field, a source port field and a target device port field of a packet of the predefined sequential triplet into a histogram table field as an ordered four-tuple; hashing the ordered four-tuple; and using the hashed ordered four-tuple as a histogram location index; and generating an alert if the predefined triplet of packets is detected and the triplet packets are each relevant to a source address;

wherein the triplet comprises an initial SYN packet originating from the source address, a next sequential SYN/ACK packet issuing from a target device address in response to the SYN packet, and a last sequential RST packet originating from the source address in response to the SYN/ACK packet.

Claims 26-29. (Cancelled)

30. (Presently Amended) A method to protect devices from malicious attacks launched on a computer network inclu~~ding the acts of~~ comprising:

providing on a device to be protected a software program that monitors packets, the software program includes a table containing codes whose values represent detection of one of the predefined set of packets and at least one source address associated with at least one of the codes, each of the predefined sequential triplet packets comprising a source address field, a target device address field, a source port field and a target device port field;

dynamically updating a histogram by concatenating a source address field, a target device address field, a source port field and a target device port field of a packet of the predefined sequential triplet into a histogram table field as an ordered four-tuple; hashing the ordered four-tuple; and using the hashed ordered four-tuple as a histogram location index; and

issuing an alert if a predefined sequential triplet of TCP/IP protocol packets are detected and the triplet packets are each relevant to a source address;

wherein the triplet comprises an initial SYN packet originating from the source address, a next sequential SYN/ACK packet issuing from a target device address in response to the SYN packet, and a last sequential RST packet originating from the source address in response to the SYN/ACK packet.

31 36. (Cancelled).

37. (Presently Amended) The method of claim-[~~36~~] 1, wherein detecting the predefined sequential triplet comprises:

concatenating source address, target device address, source port and target device port fields of the SYN packet in a source address-target device address-source port-target device port first order four-tuple and initializing the state code field;

concatenating source address, target device address, source port and target device port fields of the SYN/ACK packet in a reflection of the first order in a target device address-source address-target device port-source port reflected order four-tuple and incrementing the initialized state code field; and

concatenating source address, target device address, source port and target device port fields of the RST packet in a first order four-tuple and incrementing the incremented state code field into the alert value.

38. (Previously added by amendment) The method of claim 37, comprising:
starting a purge time period;
purging the state code field upon a lapse of the purge time period.

39. (Previously added by amendment) The method of claim 37, wherein detecting the next sequential SYN/ACK packet comprises matching a look-up table key source address to the SYN/ACK source address field.

40. (Presently Amended) The method of claim [~~26~~] 25 further comprising blocking future packets comprising the source address, the target device address and a target device port address.

41 (Presently Amended) The method of claim [~~26~~] 25 further comprising rate-limiting flows of packets comprising the source address.

42. (Cancelled)

43. (Presently Amended) The method of claim-[~~42~~] 25, wherein detecting the predefined sequential triplet comprises:

concatenating source address, target device address, source port and target device port fields of the SYN packet in a source address-target device address-source port-target device port first order four-tuple and initializing the state code;

concatenating source address, target device address, source port and target device port fields of the SYN/ACK packet in a reflection of the first order in a target device address-source address-target device port-source port reflected order four-tuple and incrementing the initialized state code; and

concatenating source address, target device address, source port and target device port fields of the RST packet in a first order four-tuple and incrementing the incremented state code into an alert value.

44. (Previously added by amendment) The method of claim 43, comprising:
starting a purge time period;
purging the state code upon a lapse of the purge time period.

45. (Previously added by amendment) The method of claim 43, wherein detecting the next sequential SYN/ACK packet comprises matching a look-up table key source address to the SYN/ACK source address field.

46. (Presently Amended) The method of claim [~~35~~] 30 further comprising blocking future packets comprising the source address, the target device address and a target device port address.

47 (Presently Amended) The method of claim [~~35~~-] 30 further comprising rate-limiting flows of packets comprising the source address.

48. (Cancelled)

49. (Presently Amended) The method of claim-[~~48~~] 30, wherein detecting the predefined sequential triplet comprises:

concatenating source address, target device address, source port and target device port fields of the SYN packet in a source address-target device address-source port-target device port first order four-tuple and initializing a state code;

concatenating source address, target device address, source port and target device port fields of the SYN/ACK packet in a reflection of the first order in a target device address-source address-target device port-source port reflected order four-tuple and incrementing the initialized state code; and

concatenating source address, target device address, source port and target device port fields of the RST packet in a first order four-tuple and incrementing the incremented state code into an alert value.

50. (Presently Amended) The method of claim 49, comprising:

starting a purge time period; and

purging the state code upon a lapse of the purge time period.

51. (Previously added by amendment) The method of claim 49, wherein detecting the next sequential SYN/ACK packet comprises matching a look-up table key source address to the SYN/ACK source address field.

REASONS FOR ALLOWANCE

2. The following is an examiner's statement of reasons for allowance: The prior art does not provide for, nor suggests providing for, an intrusion detection system utilizing a histogram tables which keep track of sessions utilizing a four-tuple hash (i.e. source address, source port, destination address, destination port) which is used as an index into the table. Once the index is found, the code value is initialized into a first state if the packet first received is a SYN packet, incremented into a second state if a packet received is a SYN/ACK packet, and incremented into a third state if the packet received is a RST packet as described in the specification. Once a RST packet has been received, an alarm message commensurate with the configuration with the system is generated once the RST state is received. For these reasons, in conjunction with the other limitations of the independent claims, puts this case in condition for allowance.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joseph E. Avellino whose telephone number is (571) 272-3905. The examiner can normally be reached on Monday-Friday 7:00-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David A. Wiley can be reached on (571) 272-3923. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Joseph E. Avellino/
Joseph E. Avellino, Examiner
December 15, 2007